Integrated Technology Security Assurance Plan

This plan documents the Integrated Technology and Security Assurance Plan and Procedures to protect the information generated or provided as part of on-going operations of the Ames Laboratory, as may be required under federal law and/or with management and operations requirements under the Laboratory's DOE contract. This plan also replaces the Export Control Plan 10100.001 Revision 3 dated 2/15/2012.

1.0 APPROVAL RECORD

- Reviewed by: Human Resources Manager (Diane Muncrief)
- Reviewed by: Information Systems Manager (Diane Den Adel)
- Reviewed by: Purchasing & Property Services Manager (Andrea Spiker)
- Approved by: Environment, Safety, Health & Assurance Manager (Tom Wessels)
- Approved by: Chief Operations Officer (Mark Murphy)
- Approved by: Associate Laboratory Director for Sponsored Research (Debra Covey)
- Approved by: Assistant Director, Strategic Planning (Cynthia Jenks)
- Approved by: Chief Research Officer (Duane Johnson)
- Approved by: Interim Deputy Director (Tom Lograsso)
- Approved by: Director (Director)
- Reviewed by: Ames Site Office Manager (Cynthia Baebler)

The official approval record for this document is maintained in the Training, Documents & Records Office in 151 TASF.

2.0 REVISION/REVIEW INFORMATION

One; this is the first revision of this plan. Future revision descriptions for this document will be made available from and maintained by the author.

3.0 POLICY

It is the policy of the Ames Laboratory to adhere to Bureau of Industry and Security (BIS), and International Traffic in Arms (ITAR) regulations, DOE orders and policies as they pertain to the protection, both physical and electronic, of Ames Laboratory developed technologies including intellectual property and data.

Compliance with this plan is the responsibility of each Ames Laboratory employee.

4.0 PURPOSE AND SCOPE

As a national laboratory and residing on the campus of Iowa State University, the Ames Laboratory hires, collaborates and interacts with foreign nationals and nations worldwide. The Ames Laboratory does not conduct classified research, has no classified documents and does not sponsor any security clearances. While the Laboratory's major thrust is fundamental research conducted to advance general knowledge, practical applications can or may develop from this research. These applications may be sensitive and subject to controls.

The purpose of this plan is to outline the roles and responsibilities of Laboratory employees in regards to the protection of Laboratory intellectual assets, combining into a single plan the protection of such assets taken from the Integrated Safeguards and Security, Cyber, and Export Control plans, policies and procedures.

The safeguard procedures outlined in this plan are the responsibility of all research and support staff that may have contact with or be affected by the information contained within the Laboratory's documentation.

5.0 ROLES AND RESPONSIBILITIES

5.1. Director and Deputy Director

Both the Director and Deputy Director are responsible for the implementation and oversight of all matters related to safeguards and security as well as active members of the Executive Council. The Safeguards and Security Program Director and Manager report directly to the Deputy Director.

5.2. Safeguards and Security Program Manager

The Laboratory's Safeguards and Security Program Manager has responsibility for S&S related budgetary issues, development of the Site Security Plan, and overview and coordination of S&S functional areas.

5.3. Associate Laboratory Director for Sponsored Research Administration and Export Control Manager

The Associate Laboratory Director for Sponsored Research Administration (ALD) also serves as the Export Control Manager for the Ames Laboratory and is a member of the Laboratory's Executive Council. The Export Control manager is a member of the DOE's Export Control Coordinators' Organization (ECCO) and a member of the Laboratory's Safeguards and Security Oversight Committee.

The Associate Laboratory Director is responsible for:

- Maintaining the Laboratory's Sensitive Technology List.
- Reviewing all ongoing and proposed research for export control implications and utilizing the Laboratory's preproposal form, documenting any export control requirements that must be completed prior to commencement of work on a new project.
- Reviewing and approving all foreign visits and assignments for export control implications. These forms are forwarded to Human Resources for processing/document verification and data entry into Ames Laboratory's database.
- Performing export control reviews on Foreign Travel Authorization forms, for possible export control issues as requested by the COO, and material order requests through the MPC and other researchers from foreign entities.
- Preparing and submitting export control licenses to the Department of Commerce for approval, when needed.
- Educating and reminding staff as to their responsibilities under Export Control Regulations.

5.3.1 Intellectual Property Coordinator

Reporting to the ALD, the IP Coordinator is responsible for working with staff to document intellectual property disclosures, educate staff and answer inquiries regarding disclosures, patents, and patenting. The IP Coordinator works with DOE-Chicago to discuss any potential IP issues regarding research agreements, meets with internal and external representatives regarding Laboratory IP, serves as a liaison with ISURF, assists HR with Laboratory notebook guidelines, training, and issues, administers the Laboratory's inventor incentive program.

5.4. Chief Operations Officer

The Chief Operations Officer is responsible for:

- Serving as a backup to the Export Control Officer in her/his absences.
- Performing the initial review of form F551.1, Request for Foreign Travel Authorization

Form, for possible export control issues and Safety and Security issues which may arise, notifying the Export Control manager when items on the Sensitive Technologies List may be involved.
- Supervising OPOC FV&A.
- Is an active member of the Executive Council and the Safeguards & Security Oversight Committee.

5.4.1 Organizational Point of Contact for Foreign Visits & Assignments
The OPOC FV&A is responsible for updating forms used to gather data regarding visitors & assigned employees to Ames Laboratory who are not U.S. citizens. Inputs data in FACTS for use by OICI-Chicago. Serves as liaison with OICI-Chicago & other DHS personnel as needed.

5.5. Manager, Purchasing and Property Services Office
The Manager, Purchasing and Property Services is responsible for maintaining the High Risk Equipment list, sending overseas shipments and preparing equipment for disposal, transfer or sale.

5.6. Manager, Budget Office
The Budget Officer is responsible for notifying the ALD when a new DOE or Other Federal Agency project has been funded.

5.7. Manager, Human Resources Office
The HR Manager is responsible for:
- Facilitating the visa application process for all foreign employees with the ISU Office of International Students and Scholars and verifying visitor status.
- Providing an annual reminder on OUO and PII.

5.8. Coordinator, Documents, Records, and Training Office
The Documents, Records, and Training Coordinator is responsible for:
- Securing and protecting Laboratory notebooks utilized for research and development.
- Training of general staff in Laboratory standards and practices regarding Official Use Only (OUO) and Personally Identifiable Information (PII) and Privacy standards.

5.9. Manager, Information Systems Office
The IS Manager is responsible for:
- Providing the active Laboratory staff with a secure means of electronic storage for Sensitive Information and, as needed, internet access to said secure electronic storage offsite, as job duties require.
- Working with the EC manager and project PIs to determine appropriate protections are addressed and, if needed, a cyber-security plan is in place for the research.

5.9.1 Assistant Cyber Security Manager (ACSM)
The Assistant Cyber Security Manager is responsible for meeting with the project leader, once an agreement is established for a project, to discuss & implement moderate controls, data storage, and offsite access.

5.9.2 Cyber Security Team
The Cyber Security Team is responsible for providing the active Laboratory staff with appropriate access to Laboratory networks at a security level defined under the Cyber Security Plan. Authentication and authorization mechanisms will be implemented to restrict access to sensitive information and data storage, which will be monitored by the Cyber Security Team, as

required.

5.10. Manager, Facilities & Engineering Services

The FES manager is responsible for limiting physical access to Ames Laboratory facilities, which house computers and potentially sensitive resources, physical keys and electronic (keycard) access. The FES manager is also responsible for the Emergency Management Plan.

5.11. Employees

Employees are responsible for:

- Being actively aware of confidential, OUO, PII, EC and other such sensitive documents and data in their areas.
- Protecting and monitoring for any breach of the above documents and data under their control.
- Initiating follow-up on changes in personnel that will have access to such information with the EC Manager and for potential breaches in security with their supervisors.

6.0 PREREQUISITE ACTIONS AND REQUIREMENTS

6.1. Definitions or Vocabulary

The Ames Laboratory Sensitive Technology List: A compilation of technical subject matter or technologies at AMES that may have export control implications or that are sensitive in nature, as determined by DOE or Other entities.

The Department of Commerce Bureau of Industry and Security (BIS): Charged with the development, implementation and interpretation of U.S. export control policy for dual-use commodities, software, and technology. www.bis.doc.gov.

DOE Sensitive Subjects List (SSL): A compilation of technical subject matter or technologies that is intended to aid the Department of Energy (DOE)-complex in identifying “sensitive” information. The list identifies subjects related to the development and production of weapons of mass destruction (nuclear, chemical, and biological) and their delivery systems (including missiles), conventional weapons, and other technologies deemed significant to the national security of the United States. The SSL is an internal DOE document that is not used outside of the DOE-complex. It does NOT replace or supersede U.S. export control regulations.

Dual-use Items: Items subject to BIS regulatory jurisdiction that have predominantly commercial uses, but also have military applications.

Export Administration Regulations: The EAR is codified at 15 Code of Federal Regulations, Chapter 7. The Government Printing Office’s Export Administration Regulation Web site contains an up-to-date database of the entire Export Administration Regulations (EAR), including the Commerce Control List, the Commerce Country Chart, and a link to the Denied Persons List.

Foreign National: As defined in EAR, a foreign entity who is not a permanent resident alien nor an asylee. As defined by DOE, all non-U.S. citizens.

Fundamental Research: Basic and applied science and engineering where the resulting information is ordinarily published and shared broadly within the scientific community.

Foreign Access Central Tracking System [FACTS]: The DOE database for entry of all pending or potential foreign visits and assignments information. This information is then transmitted to AMSO Office of Intelligence and Counterintelligence for review.

High Risk Personal Property (HRPP): Property that, because of its potential impact on public health and safety, the environment, national security interests, or proliferation concerns, must be controlled and dispositioned in other than the routine manner. This order provides accountability and control requirements for only the following categories of HRPP: especially designed or prepared property; export controlled property; hazardous property; radioactive property; nuclear weapon components or weapon-like components that do not contain nuclear material as listed in DOE O 474.2; proliferation sensitive property; and firearms, ammunition, pyrotechnics, and explosives. For the purposes of this order, HRPP does not include nuclear material within the scope of DOE O 474.2.

6.2. Acronyms

ACSM - Assistant Cyber Security Manager

ALD – Associate Laboratory Director

BIS - DOC's Bureau of Industry and Security

COO - Chief Operations Officer

CRADA - Cooperative Research and Development Agreement

CSPP – Cyber Security Program Plan

DOC - Department of Commerce

DOE - Department of Energy

EAR - Export Administration Regulations

EC - Export Control

ECCN - Export Control Commerce Number

ECCO - DOE's Export Control Coordinators' Organization

FACTS – Foreign Access Central Tracking System

FES – Facilities and Engineering Services

FV&A - Foreign Visits and Assignments

FWP – Field Work Proposal

HR - Human Resources

HRPP – High Risk Personal Property

IP – Intellectual Property

IPDR – Intellectual Property Disclosure Record

IS – Information Systems

ISU - Iowa State University

ISURF – Iowa State University Research Foundation

ITAR – International Traffic in Arms Regulations

MPC - Materials Preparation Center

NIST – National Institute of Standards and Technology

OICI – Office of Intelligence and Counterintelligence

OPOC - Organizational Point of Contact

OSRA - Office of Sponsored Research Administration

OUO – Official Use Only

PI - Principal Investigator

PII – Personally Identifiable Information

PPF - Preliminary Proposal Form

S&S - Safeguards and Security

SSL – Sensitive Subjects List

STL – Sensitive Technology List

TT – Technology Transfer

WAS - Work Authorization System

WFO - Work for Others

7.0 PROGRAM/POLICY/PROCEDURE INFORMATION

As required of all U.S. entities, the Ames Laboratory complies with the U.S. export control regulations and practices, including ITAR. While the majority of work performed at the Ames Laboratory is considered “fundamental research”, (as defined within the EAR), any foreign national who is not a permanent resident alien nor an asylee will be required to have an EC review completed before gaining access to the Ames Laboratory. In addition, if the foreign national’s research duties change substantially, another EC review must occur before assuming such duties.

International shipments will require an export control review as well (see exceptions under 7.3.3.2.1.).

7.1. Sensitive Technology List

The STL provides a log/record for those in the Laboratory with a need to know & is maintained & updated by the EC Manager.

Technologies or projects are added to the STL if:

- It has an ECCN other than EAR99, or falls under ITAR.
- It falls into one of the DOE SSL categories.
- DOE has asked that the Laboratory treat the subject technologies/projects as sensitive.
- The work is for an entity that has asked that the technology/project be treated as OUO, confidential or that foreign nationals cannot work on the project.
- CRADAs (5 year protected CRADA data)

7.1.1. The STL is made available to the Safeguards and Security Oversight Committee and the OPOC FV&A.

7.2. Safeguards & Security

All requests for access to buildings and research project groups have to be in writing and signed by the Division/Program Director or Department Manager and must be triggered by an established "official business" need. This is to ensure that the individual has access only to the required room(s). Any access changes must be in writing (by memo, email, etc.) and should document the employee number, the room involved, and the first five/six digits on the back of the employee's ISU ID. In the event that the employee is issued a physical key, the key must be checked out from Facility Services or checked back in by Facility Services, as the need and permissions allow. In the event a keycard is lost, the door code can be changed to reset security practices. In the event a physical key is lost, the door lock may be replaced, as the risk assessment and security practices dictate.

7.3. Export Control

Export Control encompasses all of the research performed at the Laboratory as well as information or data that may be considered OUO or non-classified sensitive information. The EC review processes are discussed below: All EC reviews are documented using the web-based ECustoms by Visual Compliance Export Control Review application.

7.3.1. Research Projects

7.3.1.1. Out of Cycle Submissions

When a researcher proposes a new research project for funding to DOE, other Federal Agencies, or non-federal partners, s/he initiates a PPF (AL Form 10100.001) to begin the Laboratory's review process for new or ongoing work. This form provides areas for signature of appropriate Laboratory officials to make sure pertinent issues have been addressed and approved. One of these areas is Export Control. The Export Control Manager reviews the proposal for potential EC implications; if any exist (i.e. the proposed work will not be "fundamental research"), a notation is made on the PPF for follow-up review when the proposal is funded.

7.3.1.2. In-cycle Proposals

All proposals that are included in the Laboratory's Annual Budget Submission in the Work Authorization System are reviewed by the EC Manager and authorized. If there are EC requirements, this is noted on the WAS Checklist form that goes to the Budget Office. If required, an EC review is performed and documented and a license is processed for approval by DOC.

7.3.1.3. Funded Research

For any proposal that had EC implications noted on its PPF, when the Laboratory receives funding for that work, the Budget Officer notifies the Export Control Manager. The Principal Investigator is then asked to meet with the EC Manager to perform an export control review of the project to determine if any part of the project would be subject to the EAR and signed by both the PI and EC Manager.

If the research falls under the EAR, then the researcher is asked additional questions, including:

- Will foreign nationals work on the project? If so, are they presently working at Ames Laboratory? What nationality are they? Is their country of origin classified as a sensitive or terrorist country?
- What controls exist for each ECCN that the research falls under?

- Do any of the foreign nationals, currently employed by the Laboratory, who will work on the project, country of origin fall under the controls?
- Do you plan to hire any new researchers to work on the project? Will they be foreign nationals?

Dependent upon the answer to these types of questions, a determination is made as to whether a License will be required, or if a License could be required dependent upon the nationality of any new hires. The PI is also informed that if s/he would want to have foreign nationals work on the project at a future date, another EC Review would need to be completed before hiring such personnel. If a License application is required, either the License will be prepared and submitted for approval, or the PI may decide to find alternate employees that are not subject to the EAR. If some or all of the research falls under the EAR, the PI is also informed that discussing the research with foreign nationals could be a deemed export, and a License would have to be requested before discussing the project with certain foreign nationals.

If a License is requested, or if the research falls under a category on the DOE Sensitive Subject list, the research is added to Ames' Sensitive Technology List for monitoring. This list is provided to the COO for his use in FV&A and Foreign Travel. If the research does not fall under the EAR, the form is filed for documentation that such review occurred.

7.3.1.4. After the completion of the review or after obtaining a license(s) (if required), the Budget Manager is notified that all EC requirements have been addressed. The Budget Manger will then allow work to commence.

7.3.2. Technology Transfer Agreements (WFO, CRADA, ACT, others)
For business proprietary information contained in fully executed technology transfer agreements, the process listed under funded research is followed. In addition, once the CRADA is signed, the researchers are reminded that if/when there is "protected CRADA data" that an EC review must occur if there are foreign nationals working on the project, or if the potential for foreign nationals to work on the project exists.

7.3.2.1. New agreements and their participants are compared to the Sensitive Technology List to assess any potential disclosure or security issues.

7.3.3. Intellectual Property
All inventions shall be documented in a Laboratory notebook procured at the Laboratory storeroom. These notebooks contain a barcode that can be tracked by the Ames Laboratory Training and Records Management office. Physical control of the notebook must be maintained to prevent unauthorized access. When not in use, the notebook must be stored in a secure container (e.g., locked desk or file cabinet) or in a location where access is limited (e.g., locked or guarded office, controlled access facility).

Inventions may also be documented electronically if adequate safeguards are taken. Electronic research data should be on the moderate enclave, where it is backed-up on a daily basis.

All IP must be disclosed via the Intellectual Property Disclosure and Record (IPDR) form. The required IPDR form can be accessed from the forms site at the Ames Laboratory's webpage, www.ameslab.gov.

Once completed, the IP Coordinator will review the form, print it, and obtain authorizing signatures. The original document will be hand-delivered or sent by first-class mail to the Iowa State University Research Foundation. A copy of the completed form is kept in the Laboratory Director's office in the locked Lektriever. Any copies maintained by the inventors are kept in a secure container or where access is limited. Any electronic copies are stored on the moderate enclave. Any hard copies produced that are not needed may be disposed of by any method which assures sufficiently complete destruction to prevent its retrieval (e.g., shredding).

All employees of the Laboratory are periodically required to complete an IP agreement that states they will protect and not disclose the Laboratory's proprietary, technical, business and financial data. All new employees, as part of their orientation training, complete an IP agreement form when starting at Ames Laboratory.

Intellectual Property Coordinator transmits safeguard standards to the EC Manager and Cyber Security Team to allow for adjustments to the standards for moderate enclave security for the applicable employees. The Cyber Security Team notifies the ACSM.

7.3.3.1. Procurement

Purchasing obtains the EC classification from vendors prior to purchasing personal property. If the personal property is classified as EC, Property Services designates as high risk in the Fixed Asset database and notifies the EC Manager. The EC Manager reviews the EC classification and notifies the PI on handling and access requirements for the asset.

7.3.3.2. Property Services

The Materials Handling department is responsible for reviewing all Shipping Orders to identify requests for foreign shipments of materials and supplies and obtaining the proper ECCN from the EC Manager, license exception or completed license application from the EC manager, for inclusion on export documents, prior to shipment (publicly available print/publication documents are exempt from this procedure).

7.4. Foreign Visits and Assignment (FV&A)

An EC review of the visit or assignment is completed on all Ames Laboratory funded foreign nationals. ISU funded individuals occupying Ames Laboratory space will have a restricted parties review performed on the individual, but it will be ISU's responsibility to determine if an EC license is needed for such individuals. If the research falls under EAR, a license will be requested from BIS before allowing the individual(s) access to controlled information. If the PI affirms that the individual(s) will only have access to "fundamental research", but the PI has past or ongoing research that falls under the EAR, and the individual(s) are from a country that the technology/information is subject to EAR, then a letter is sent to the PI reminding him/her of their responsibilities not to share any controlled information with them (DOE O 142.3A).

Foreign nationals receiving a new or extended J-1 or H-1 visa will have an Export Control review performed by the Laboratory.

When a security plan is required for a foreign visitor, an additional EC review/approval is obtained. Typically these plans are limited to 1) all visitors from terrorist supporting countries, 2) situations where the host has a clearance and his/her visitor is accessing sensitive information or is from a sensitive country, and 3) where the visitor is not a legal permanent resident and needs to access sensitive information.

7.4.1. Specific Security Plan

The Specific Security Plan is the security plan required for foreign nationals of countries that are defined as sponsoring terrorism, regardless of topic, or where the work that is being performed or to which the foreign national has access to is on the STL.

The SSP will be developed by the PI, Program Director and the OPOC FV&A in consult with the EC Manager and others, as needed. A Non-Disclosure Agreement (NDA) may be required as well as an EC license. These requirements can be obtained with the assistance of the COO and the ALD. Once developed, the OPOC will provide a copy of the SSP for review and approval by the COO, EC Manager, S&S Manager, and the host prior to the arrival of the foreign national at the Laboratory.

7.4.2. Cyber Specific Security Plan

A standard cyber security plan was developed to encompass all Foreign Nationals accessing low enclave data with the exception of those from Terrorist Countries or those foreign nationals required to have an export control license. Additional documentation is not required for Foreign Nationals in the low enclave category.

An individual cyber security plan for the following must be completed:

- Any Foreign National from a Terrorist Country
- Any Foreign National accessing Moderate Enclave data
- Any Foreign National required to have an export control license

7.4.3 DOE Office of Intelligence and Counterintelligence

If security concerns arise regarding information provided on or not disclosed on the 473, the Laboratory's COO is to be notified. COO notifies DOE OICI & Executive Council. The COO involves HR if deemed appropriate in order to address HR issues pertinent to the concerns.

7.4.4 Access through Authorized Host

Host training is required for all who will be hosting a non-U.S. citizen employed at the Ames Laboratory. The Ames Laboratory Training Office, a division of the HR Office, provides the training per AL-193 guidelines. Annual retraining of Hosts is provided by the Training Office.

Chicago Service Center monitors any potential loss of/access to sensitive information by a foreign national while being hosted. A Host will ensure compliance with required training, including safety, while hosting a foreign national. Host will inform employees in the work area about intended assignments and remind them to deflect inquiries that attempt to seek information not appropriate to the assignment, including personal information, other personnel, or government programs.

7.4.1. **Cyber Security**

The Cyber Security Program Plan (CSPP) provides an overview of the security requirements of the enclave and describes the controls in place or planned for meeting those requirements. The CSPP defines responsibilities and expected behavior of all individuals that access the system. The structured process of planning adequate, cost-effective security protection for the Laboratory's system is documented in the CSPP.

The Cyber Security Team assesses the environmental, natural, and man-made risks associated with computer and network security from external and internal perspective. These assessments weigh a potential attack to any vulnerable area. Remediation may be required to

reduce vulnerability to an acceptable level. If remediation is not cost effective or cannot be accomplished, the risk must be acknowledged and the residual risk documented.

7.4.2. Research Programs

The STL indicates to the Cyber Security Team the necessity for moderate controls, data storage, and potential offsite access needed within each identified sensitive project. Utilizing job duties and functions, the COO and the Department Managers work with IS to provide training on how to identify sensitive data and how to store/access the moderate date within system controls. IS is responsible for identifying, establishing, monitoring, and maintaining the moderate controls, once sensitive projects have been identified within the Laboratory.

7.4.3. Moderate Data

The CSPP is designed to mitigate risks associated with sensitive and protected data of value to DOE. These implemented controls specify stronger encryptions, two-factor authentication, and event logging. These controls are intended to meet the requirements for confidentiality, integrity and availability. All systems used to store moderate data must be managed and administered by IS, which applies moderate National Institute of Standards and Technology (NIST) controls. A central file server is used for accessing and storing moderate data, including research sensitive data.

7.5.2.1. Non-Administrative Functions

Moderate data should be stored on the Ames Laboratory central file systems. Home, personal devices and cloud computing storage are not approved storage locations. If the need arises to transfer moderate data off-site, encrypted storage devices (e.g. USB keys, portable hard drives, laptops) administered by IS must be used. A VPN connection will be used to access moderate data when off-site, which will require the use of a cryptocard token.

7.5.2.2. Administrative Functions

Administrative functions require a Memorandum of Understanding (MOU) and/or Interconnect Agreement (IA) between both parties that establish the communication requirements, authorize administrators of the system(s), and identify the security controls applied to the system(s).

Authentication and authorization mechanisms are used to restrict access for systems. Data stored on the moderate file server is backed up daily; weekly to an off-site storage location.

8.0 POST PERFORMANCE ACTIVITY

8.1. Export Control License

If required; an export control license will be requested. Once approved, the person(s) will have access to the research being conducted, or to item(s) shipped to the recipient. If disapproved, the PI or Program Director will be informed of this and alternative personnel will be sought to perform the work, or the item(s) will not be shipped.

8.2. Denied 473s

The OPOC FV&A documents into FACTS when an individual is denied access/authorization to participate in a project or assignment. If the individual is not the reason for the denial (no funding or the justification doesn't warrant, etc.), "Cancelled Before Approval," or "Cancelled After Approval" is noted in FACTS, with any additional "Comments" as needed. If the individual is the reason for denial, then a comment is documented as "Not authorized to work at Ames Laboratory" and the record is closed out in FACTS.

8.3. 473s Requiring a Site Security Plan

At the end of a visit or assignment requiring an SSP, the OPOC FV&A completes the FACTS entry with a noted end date and any additional "Comments" as needed.

8.4. Specific Cyber Security Plans

An individually tailored security plan as to what files may be accessed in the moderate enclave. This individually tailored security plan will be developed by the PI, Program Director and the OPOC FV&A in consult with the EC Manager and others, as needed. The Specific Cyber Security Plan is implemented by IS, under the direction of the defined parameters of the PI, Program Director and the OPOC FV&A.

9.0 Additional Information

International Traffic in Arms Regulations (ITAR). 22 CFR Parts 120-130.

U.S. Munitions List, Section 38 of the Arms Export Control Act (22 U.S.C. 2778).

Export Administration Regulations. 15 Code of Federal Regulations, Chapter 7.

DOE Sensitive Subjects, Sensitive Countries and Terrorist Countries Lists dated June, 2001.

ECustoms web based system by Visual Compliance (www.visualcompliance.com)

Cooperative Research and Development Agreements Order and Manual -DOE O 483.1-1 and DOE M 483-1-1.

Work for Others Program and Process Manual – DEAR 970.5217-1 and DOE M 481.1-1.

Cyber Security, additional informational information on AMES policy (http://www.ameslab.gov/operations/is/faq/how-should-moderate-data-be-accessed)

Site Security Plan 10200.007 Rev 7

Integrated Safeguards and Security Management 10200.029 Rev 1

Foreign Visits & Assignments, DOE O 142.3 A

10.0 Attachments

Attachment 1. Process Flowchart

Attachment 1